(19) Canadian Intellectual Property Office
An Agency of Industry Canada

Office de la Propri,t, Intellectuelle du Canada
Un organisme d'Industrie Canada

(11) CA 2 329 311 (13) A1

(40) 28.10.1999
(43) 28.10.1999

(12)

(21) 2 329 311

(22) 21.08.1998

(51) Int. Cl.6: G07C 9/00, G07F 7/10, H04Q 7/38

(85) 19.10.2000

(86) PCT/DE98/02457

(87) WO99/54851

(30) 198 17 770.4 DE 21.04.1998

(71) SIEMENS AKTIENGESELLSCHAFT,
Wittelsbacherplatz 2
D-80333, MUNCHEN, XX (DE).

(72) KARMANN, KLAUS-PETER (DE).

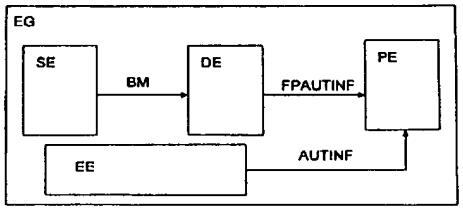
(74) FETHERSTONHAUGH & CO.

(54) APPAREIL ELECTRONIQUE ET PROCEDE POUR L'AUTHENTIFICATION D'UN UTILISATEUR DE CET APPAREIL

(54) ELECTRONIC DEVICE AND METHOD FOR THE AUTHENTICATION OF A USER OF SAID DEVICE

(57)

The inventive device comprises sensors (SE) for detecting biometric characteristics BM (e.g. finger pints) and an input device for inputting authentication data AUTINF (e.g. PIN). A data processing device (DE) of the inventive device determines authentication information FPAUTINF from the biometric characteristics BM. Said information is tested by the same testing device PE which tests the authentication information AUTINF to be input via the input device EE. As a result, the device EG can be used by different users and in the same manner as devices without sensors for biometric characteristics. The authentication rules (e.g. for mobile telephones and SIM cards) do not have to be changed in order to permit an authentication using biometric characteristics.



OPIC
OFFICE DE LA PROPRIÉTÉ INTELLECTUELLE DU CANADA

CIPO
CANADIAN INTELLECTUAL PROPERTY OFFICE

(12) (19) (CA) **Demande-Application**

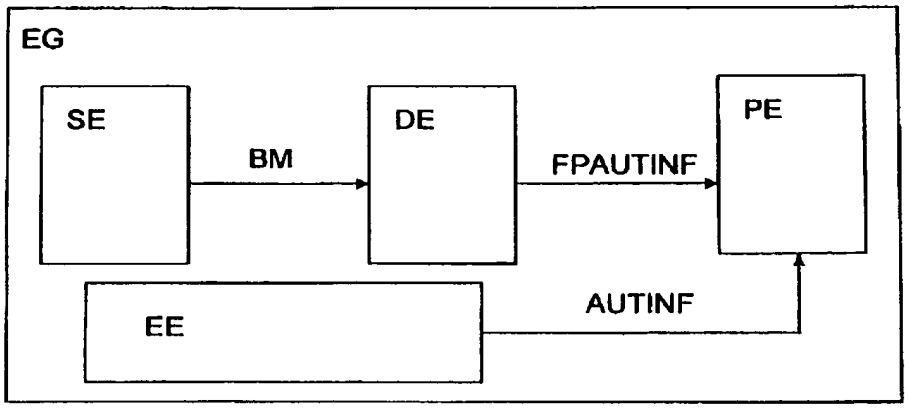
(21) (A1) **2,329,311**
(86) 1998/08/21
(87) 1999/10/28

(72) KARMANN, KLAUS-PETER, DE
(71) SIEMENS AKTIENGESELLSCHAFT, DE

(51) Int.Cl.[6] G07C 9/00, H04Q 7/38, G07F 7/10
(30) 1998/04/21 (198 17 770.4) DE

(54) **APPAREIL ELECTRONIQUE ET PROCEDE POUR L'AUTHENTIFICATION D'UN UTILISATEUR DE CET APPAREIL**

(54) **ELECTRONIC DEVICE AND METHOD FOR THE AUTHENTICATION OF A USER OF SAID DEVICE**



(57) L'appareil comprend des détecteurs (SE) pour la détection de caractéristiques biométriques BM (par exemple, empreintes digitales) et un dispositif d'entrée, pour l'introduction de données d'authentification AUTINF (par exemple PIN). Un dispositif de traitement de données (DE) de l'appareil calcule, à partir des caractéristiques biométriques BM, les informations d'authentification FPAUTINF qui sont contrôlées par le même dispositif de contrôle PE que pour les informations d'authentification AUTINF à entrer via le dispositif d'entrée EE. L'appareil EG peut ainsi être utilisé par différents utilisateurs et de la même façon que les appareils sans détecteurs pour des caractéristiques biométriques. Les règles d'authentification (par exemple pour la téléphonie mobile via cartes SIM) ne doivent par être changées pour permettre une authentification via des caractéristiques biométriques.

(57) The inventive device comprises sensors (SE) for detecting biometric characteristics BM (e.g. finger pints) and an input device for inputting authentication data AUTINF (e.g. PIN). A data processing device (DE) of the inventive device determines authentication information FPAUTINF from the biometric characteristics BM. Said information is tested by the same testing device PE which tests the authentication information AUTINF to be input via the input device EE. As a result, the device EG can be used by different users and in the same manner as devices without sensors for biometric characteristics. The authentication rules (e.g. for mobile telephones and SIM cards) do not have to be changed in order to permit an authentication using biometric characteristics.

Abstract

Electronic device and method for the authentication of a user of said device

The device has sensors (SE) for detecting biometric characteristics BM (for example fingerprints) and an input means for the input of authentication data AUTINF (for example a PIN). A data-processing means (DE) of the device determines from the biometric characteristics BM authentication information FPAUTINF, which is checked by the same checking means PE as the authentication information AUTINF to be input via the input device EE. As a result, the device EG can be used by different users and in the same way as devices without sensors for biometric characteristics. The authentication rules (for example for mobile phones via SIM cards) do not have to be changed in order to permit an authentication by means of biometric characteristics.

GR 98 P 1550

Description

Electronic device and method for the authentication of a user of said device

Very different types of electronic device for which a user has to be authenticated before it is used are known. Important examples are computers in various configurations (devices for information processing) and telecommunication devices, such as mobile phones for example. Some devices are generally protected against unauthorized use, for example by a password; in the case of other devices, only certain functions are protected against unauthorized access (for example by a so-called Personal Identification Number, PIN). This also includes the protection of access to certain data or services, even if they are not made available by the device but by other devices in a computer network or communications network.

No doubt the most frequent type of input of authentication information today is input via a keyboard or keypad of the device. After input, the correctness of the information input, and consequently the authorization of the user carrying out the input, is checked by a checking means in the device or in a computer network or communications network. In the case of mobile phones conforming to the GSM standard, this takes place by a data-processing means on the so-called SIM card of the device checking whether the PIN input matches the information stored on the SIM card. If this is the case, the SIM card enables the mobile phone for use. The security of the telephone customer is enhanced here by the fact that the GSM standard does not allow the PIN to be stored in the device but only in encrypted form on the SIM card.

For some time, technologies which allow other forms of user authentication have been available. These technologies are based on the detection of user-specific biometric characteristics by special sensors. Sensors for fingerprint detection are an important example of this. Other biometric characteristics, such as the texture of the retina of the human eye or the characteristics of a human voice for example, are likewise already used in some devices.

The characteristics detected by the sensors are usually compared in a data-processing means of the device or of a communications network with the known characteristics of an authorised user, and if they coincide sufficiently, access to the desired service, the required data or the chosen device function is enabled.

In some types of device, it appears to be advisable to combine the two types of authentication mentioned with one another. For example in the case of mobile phones, it is undoubtedly desirable not only that they can be used by their owner by means of a fingerprint sensor, but also that other persons who have been notified of the PIN or who would like to use the device with their own SIM card are in a position to use it within the limits of the authorization to which they are entitled. In addition, the authentication by means of a fingerprint could occasionally fail or not be possible, for example because the hands of the user are soiled or the user is wearing gloves. For these or similar reasons, it is desirable or necessary that one or more users of a device can authenticate themselves on it by different means. Biometric authentication is to be possible in these cases along with authentication by PIN input. In the case of mobile phones conforming to the GSM standard, it is additionally the case

that the standard prescribes the possibility of authentication by PIN input as mandatory.

It follows from the situation described that use of conventional biometric authentication methods is not possible in the case of mobile phones conforming to the GSM standard, because PIN authentication with the SIM card is a mandatory requirement for them for reasons of compatibility with the GSM standard alone. The at first seemingly obvious possibility of storing the PIN in the device and transferring this stored PIN to the SIM card for checking purposes if there is a successful outcome of the check to ascertain whether the detected fingerprint coincides with the stored fingerprint of an authorized user is discounted because storage of the PIN in the mobile phone anywhere else than within the SIM card is prohibited by the GSM standard for security reasons. Biometric authentication would consequently only come into consideration in these cases as an additional safeguard. Such an additional safeguard is not required, however, in view of the high security of the authentication of the PIN input and would probably also not be accepted by many users.

The invention is therefore based on the object of specifying a technical teaching which allows the combination of a biometric user authentication with an authentication by PIN input even in the case of mobile phones conforming to the GSM standard or in similar circumstances, it being intended for one form of authentication to be sufficient in each case. The user is consequently to have the choice of which type of authentication he wishes to use. It is conceivable, however, that a specially distinguished user (for example the owner of the device) is given the possibility of setting the logic AND operation of the two types of authentication on the device.

This object is achieved by a device or a method according to one of the patent claims.

The invention provides that biometric characteristics of the user are detected by a sensor means and information serving for authentication is determined with the aid of mathematical methods from the detected biometric characteristics. As a result, authentication information which can be checked by the same checking means as authentication information input by the user via an information input device (for example a keyboard or keypad) is obtained at the end of the evaluation of the biometric characteristics. In the simplest case, the result of the evaluation of the fingerprint is the same PIN which users could also have input via the keyboard or keypad. This PIN is not stored in the device, however, but is calculated from biometric characteristics of a user detected by a sensor means.

This type of evaluation of the biometric characteristics detected by a sensor means makes this type of authentication equivalent in outcome to the authentication by means of keyboard or keypad input, and the customary interface for checking the validity of the authentication information can remain unchanged. In particular, it is not necessary for any requirements prescribed by standards to be changed. The two methods of authentication can be used alongside one another without any difficulties; the user has at any time and in every situation the free choice between the two methods. It is of course also possible to use both in an AND combination, in which only the user who successfully negotiates the two authentication paths is given access.

The invention is described in more detail below on the basis of preferred exemplary embodiments and with the aid of figures.

Figure 1 shows an exemplary embodiment of the invention in which all the methods and means are integrated in one device.

Figure 2 shows an exemplary embodiment of the invention in which the checking means is not located within the device.

Figure 3 shows an exemplary embodiment of the invention in which a display device for the display of authentication information is integrated in the device.

A quite specific but important embodiment of the invention is a mobile phone conforming to the GSM standard, which has a fingerprint sensor for user authentication. This fingerprint sensor is a special case of the sensor means (SE) represented in Figure 1. If a user of the device (EG) places a finger on this fingerprint sensor and the device is awaiting an authentication, such as the input of a PIN or super PIN or PIN2 (partly manufacturer-dependent) for example, the fingerprint sensor detects the corresponding biometric characteristics (BM) of the user concerned and passes them to a data processing means (DE).

In the case of the GSM mobile phone, this data processing means is the processor already present in any case in the mobile phone in conjunction with software running on it. On the other hand, however, the fingerprint sensor (or more generally: the sensor means) could also have its own processor unit, on which a special software performing the fingerprint detection runs, so that, in the sense of this invention, the data processing means is fully or partly integrated into the

sensor means. Since the fingerprint detection itself, as well as other methods of detecting biometric characteristics and their realization on data processing means of different configurations (and partitioning into subsystems or assembly from known hardware modules), are sufficiently known to a person skilled in the art, this part of realizing the invention no doubt does not present any particular problems.

According to the present invention, this data processing device then determines information suitable for the authentication of the user from the detected biometric characteristics. In the simplest case, this is the PIN (or PIN2 or the like) of the user - accepted as entitled - stored in an encrypted form on the SIM card. This PIN is then transferred to the SIM card for checking in the same way as if it had been input by the user via the numeric keypad (information input device) of the mobile phone. The checking process known to every person skilled in the art and provided in the GSM standard then proceeds in the checking means of the mobile phone (SIM card, if appropriate in conjunction with the data processing means of the device). If the authentication information FPAUTINF) is correct, i.e. coincides with the PIN stored on the STM card, the device function protected by the authentication (for example network access, etc.) is enabled.

A decisive advantage of the solution according to the invention described is that the fingerprint detection in the case of the authorized user leads to transfer of the user's PIN to the SIM card, since this allows the security requirements prescribed by the GSM standard to remain completely unchanged. Other, at first perhaps seemingly obvious solutions do not have this attribute. In any event, any other solution would require either an additional input of the PIN via the keypad or a way of avoiding or changing the

GSM standard. An additional input of the PIN via the keypad would only be meaningful if the fingerprint detection were conceived as an additional security measure in addition to the PIN input.

Such an additional authentication is of course also possible with the present invention. In this case, it would be necessary for the authentication information determined from the sensor data not to be transferred to the SIM card. Instead of this, a false PIN could, for example, be deliberately sent to the SIM card or an input error or abnormal termination of the input or the like could be simulated. The SIM card would then again request PIN input. If the PIN input coincides or is compatible with the one determined, the data processing means (DE) could transfer this PIN to the SIM card, whereupon the latter would provide the enabling function.

Of course, the PIN determined from the sensor data does not have to be identical with the SIM card PIN. If the standard or - in the case of other devices - the respectively relevant security protocols allow, the checking means could also check two different items of authentication information to ascertain whether they match one another.

In the case of other devices, which are not subject to the GSM standard, the authentication information FPAUTINF calculated from the sensor data could, even in the case of authentication by sensor data alone (that is to say independently of and along with PIN input), be different from the authentication information AUTINF input via a keypad, as long as the checking means detects that the two match in the sense that they both refer to the authorized user.

In principle, all mathematical representations (functions) which assign to a fingerprint or other BM a PIN or some other form of (generally alphanumerically encoded) authentication information AUTINF and satisfy the following conditions come into consideration as methods of calculation for authentication information FPAUTINF from a BM:
a) sufficiently similar BMs lead to the same authentication information FPAUTINF;
b) sufficiently different BMs lead to different authentication information FPAUTINF.
c) it is virtually impossible for an unauthorized user to determine (for example guess) the authentication information FPAUTINF from the BM or without knowledge of the BM.

The condition a) is intended to ensure that the fingerprint detection is sufficiently robust with respect to minor disturbances. Otherwise, the rejection rate of authorized users would be too high. Condition b) ensures that fingerprints of different users lead to different authentication information FPAUTINF with an adequately high degree of probability. The significance of condition c) is obvious.

A person skilled in the art is familiar with various mathematical representations which satisfy these requirements (possibly to a greater or lesser extent). A representation with these attributes is provided by so-called vector quantization. This method, which is actually known to a person skilled in the art, is to be explained here only to the extent which appears to be required for an understanding of the invention.

If this method is applied for the purposes of the present invention, it is firstly presupposed that the biometric

characteristics detected by the sensor means can be brought into the form of a so-called characteristic vector. This assumption is not a restriction in practice, since the sensor data can always be represented as an ordered n-tuple of n measurement data (characteristic vectors). The characteristic vectors form an n-dimensional space. In this space, a set of characteristic vectors (codebook vectors) would exist and a degree of disparity (degree of similarity for biometric characteristics) would be defined. For each sample vector there is in this space a cell, which is defined by the rule that, for each characteristic vector in a cell, the sample vector of this cell is the nearest sample vector in the sense of this degree of disparity.

Each sample vector is assumed to be assigned an item of information suitable in principle for authentication. A sample vector is assigned the correct authentication information (for example the actual PIN). It is obvious from these explanations that the determination of the nearest sample vector to a sample vector which corresponds to the detected sensor data leads to the correct information (actual PIN) in the case of the authorized user and otherwise supplies false authentication information. The error rates of this method can be optimized if it is ensured that the characteristic vector associated with the biometric characteristics of the authorized user is one of the sample vectors. This can be achieved by the system adapting itself to the biometric characteristics of the authorized user (codebook adaptation) in an initialization phase.

The vector quantization is not the only method which can be used in conjunction with the invention. A person skilled in the art is familiar with other methods, which therefore do not have to be explained here.

If the literal sense is taken as a basis - the calculation of the authentication information FPAUTINF from the biometric characteristics of a user by vector quantisation actually also involves a "storage of the PIN" in the device, since each sample vector of the codebook is indeed assigned an item of authentication information (FPAUTINF) that is possible in principle. However, in virtually all cases (apart from one, namely that of the sample vector of the authorized user) this is not really suitable for authentication. For example, in the case of a five-place alphanumeric PIN, in the ideal case all conceivable PINs, and for each one a sample vector, are therefore stored in such a way that only if there is sufficiently accurate detection of the sample vector in the sensor can the valid PIN be addressed. Although the correct PIN is therefore accordingly "stored in the device", it is lost among the great number of conceivable PINs, and can only be found for the person with the correct biometric characteristics. This state of affairs is not intended when the standard prohibits the storage of the PIN in the device.

In the case of the GSM standard, the storing of the PIN in the device is not allowed. Often, however, a change of the PIN is necessary, for example because it has become known to a third party. If, however, the PIN is determined from the fingerprint (i.e. calculated), this initially appears to be impossible, since it is not possible to change a fingerprint or other biometric characteristics. In order nevertheless to give the user the possibility of changing his PIN, the invention provides in a preferred embodiment that, instead of only one method of calculation, a whole set of such methods are available in the device. Each individual method of calculation could be assigned a consecutive number, so that a user authorized to do so could at any time change the method used.

Since each method (M1,...,Mn) calculates a different PIN (FPAUTINF1,...,FPAUTINFn) for one and the same fingerprint (BM), the user can select from as many PINS as there are different methods for their calculation.

This embodiment of the invention can likewise be realized with vector quantization, although indeed not just one codebook but a number of codebooks of sample vectors are to be provided. Each codebook has a number and can be selected via this number. Other methods possibly depend on a parameter. If this parameter is changed, a different mathematical representation is obtained. If the dependence on this parameter is sufficiently complex, it becomes virtually impossible to guess how the authentication information changes when the parameter changes.

Certain types of neural networks (for example so-called multi-layer perceptrons) are suitable for realizing representations of this type. In the case of solutions based on such neural networks, the PIN is actually not stored anywhere as a sequence of characters but merely (implicitly encrypted) in the network architecture and in the weight coefficients.

This implementational variant of the present invention appears to be of interest in particular with regard to the fact that many people require a series of different passwords for quite different purposes or devices. It is becoming increasingly more difficult to remember these many passwords. If a number of methods (M1,...Mn) (mathematical representations) are used for calculating a number of items of authentication information (FPAUTINF1,...,FPAUTINFn) from a single characteristic vector (or set of sensor data), this problem is reduced to the detection of user-specific inalienable biometric characteristics by suitable sensors.

For the selection of a certain method, all that is necessary is to input an identification number of such a method in a context of the user interface to be provided for this purpose. As a result, the data processing means can be correspondingly set up by software.

Of course, the biometric characteristics of a number of people could also be linked with the correct PIN or with a number of correct PINs. If, as an exception, the device is to be usable only for one person, i.e. with only just one SIM card, the enabling function may be additionally linked with further safety mechanisms such as device codes, etc. The invention allows any kind of flexibility here, together with the highest security and compatibility with the standard.

Specifically if a PIN is changed, a further useful embodiment of the invention, in which a display is provided for displaying an item of authentication information, may be helpful. A display of this type is already present in any case on many devices of this type and can therefore also be used for these purposes. If a user wishes to change his authentication information (AUTINF), for example the PIN, to be input via the keypad and matching the SIM card or stored on it, it is possible in the case of some methods of calculation that not all the conceivable character-digit combinations are available to him as PINs, for example because the codebook is smaller than the number of all conceivable PINs. In this case, changing the parameter of the method of calculation used (for example changing the codebook number, or changing a parameter of a neural network) is sufficient to change the assignment of the PINs to the sample vectors and consequently the PIN assigned to its individual sample vector. After that, he could not change the PIN on the SIM card (or more generally: the PIN

to be input) in the same sense without knowing it. This is necessary, however, for further use in the sense of our object. The changed PIN is therefore preferably divulged to the authorized user by a corresponding, possibly one-off, brief display of this PIN after the change on a display of the device. Other solutions (for example mailing the new PIN) are conceivable.

The invention is of course not restricted to mobile phones, in particular not to mobile phones conforming to the GSM standard. It is quite evident to a person skilled in the art from the present description how the invention is to be realized in the case of other devices or systems.

In particular, the invention is not restricted to the case in which the checking unit (PE) is integrated into the device. Figure 2 shows the important case of a device which is connected, for example via a communications network, to at least one other device, in which the checking means is located. However, even the data processing unit or that part of the data processing unit (DE) which is responsible for the calculation of the authentication information FPAUTINF from the biometric characteristics BM of the user does not necessarily have to be located in the device. Of course, the device does not have to have an integrated sensor means (SE) or an integrated keyboard or keypad (EE). These means could of course also be connected to the device in the form of external modules. These embodiments of the invention are intended to be protected by the method claims.

Patent claims

1. An electronic device (EG), in particular a device for information processing or for telecommunication, with
a) a sensor means (SE) for detecting biometric characteristics (BM) of a user of the device, in particular for detecting fingerprints,
b) a data-processing means (DE) for determining information (FPAUTINF) serving for the authentication of a user from detected biometric characteristics,
c) an input means (EE) for the input of information with the possibility of using this input means for the input of information (AUTINF) serving for authentication,
d) a checking means (PE) for checking the determined or input authentication information and for enabling device functions for this user if the check is successful.

2. The device as claimed in claim 1, the data-processing means (DE) of which can be set up in such a way that the authentication information (PIN) to be input via the input means for successful authentication checking is identical to authentication information (FPPIN) determined from the biometric characteristics of an authorized user.

3. The device as claimed in one of the preceding claims, the data-processing means (DE) of which has a number of methods (M1,...,Mn) for determining from the detected biometric characteristics of a user information (FPAUTINF1,...,FPAUTINFn) serving for authentication of this user.

4. The device as claimed in claim 3, the data-processing means of which permits an authorized user to select from the

number of methods for determining authentication information from biometric characteristics a method desired by him.

5. The device as claimed in one of the preceding claims with means for displaying authentication information (FPAUTINF) determined from biometric characteristics of a user.

6. A method for the authentication of a user of a device, in which the user has the possibility of authenticating himself with the aid of user-specific biometric characteristics or by input of authentication information via an information input device, in the first case biometric characteristics of the user being detected by a sensor means and information serving for authentication being determined from the detected biometric characteristics and checked by a checking means, and in the second case the authentication information input by the user via the input device being checked by the same checking means.

7. The method for the authentication of a user of a device as claimed in claim 6 with the following steps:
a) the determination of a characteristic vector from measurement data of a sensor means,
b) a vector quantization of the characteristic vector determined, and
c) checking of authentication information belonging to the result of the vector quantization.

Fetherstonhaugh & Co.
Ottawa, Canada
Patent Agents

FIG 1

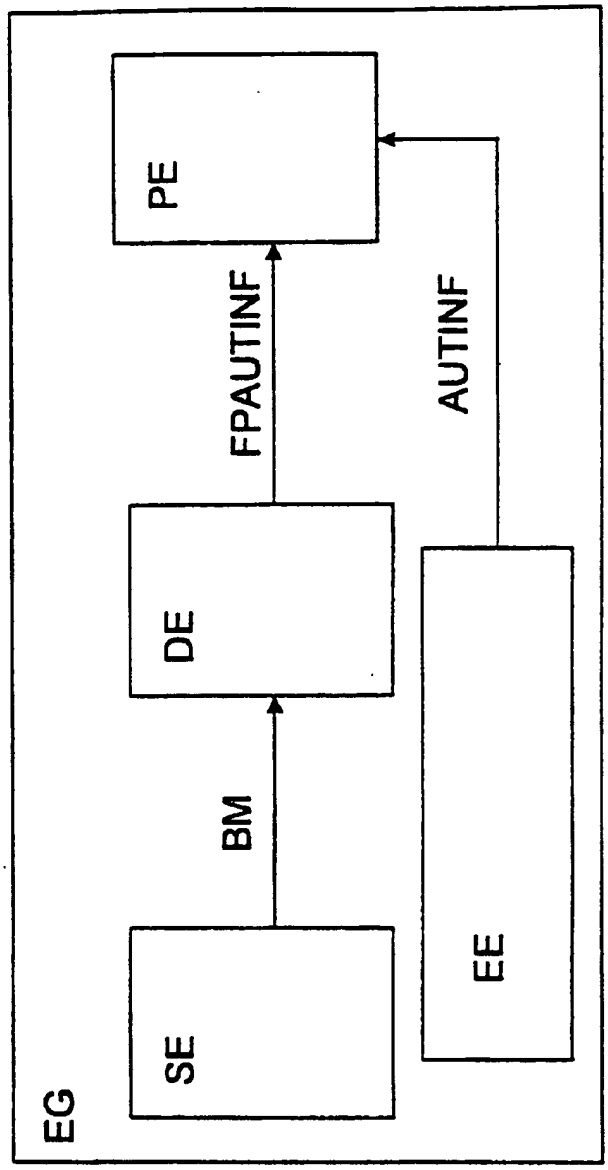


FIG 2

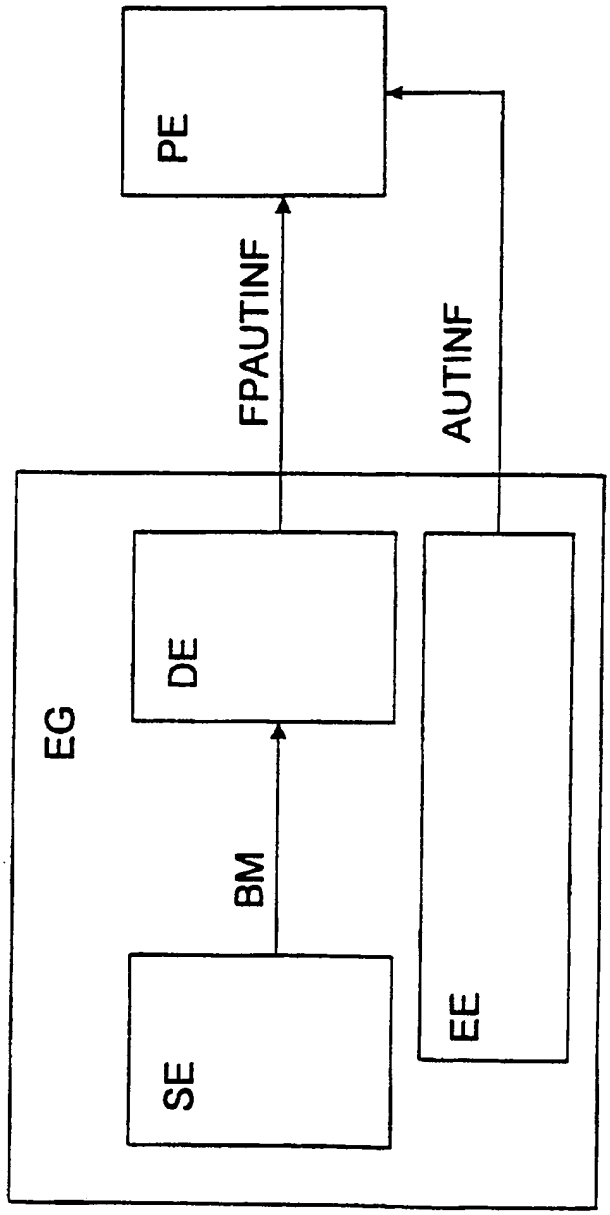


FIG 3